State of California - Department of Social Services
DUTY STATEMENT

EMPLOYEE NAME:	
VACANT	
CLASSIFICATION:	POSITION NUMBER:
INFORMATION TECHNOLOGY SPECIALIST I	721-1402-955
DIVISION/BRANCH/REGION: *(UNDERLINE ALL THAT APPLY)*	BUREAU/SECTION/UNIT: *(UNDERLINE ALL THAT APPLY)*
ISD/Information Security and Privacy Office	PRCB/Monitoring and Response Unit
SUPERVISOR'S NAME:	SUPERVISOR'S CLASS:
Roy Chang	INFORMATION TECHNOLOGY SUPERVISOR II

SPECIAL REQUIREMENTS OF POSITION *(CHECK ALL THAT APPLY)*:

- ☐ Designated under Conflict of Interest Code.
- ☐ Duties require participation in the DMV Pull Notice Program.
- ☐ Requires repetitive movement of heavy objects.
- ☐ Performs other duties requiring high physical demand. *(Explain below)*
- ☐ None
- ☑ Other *(Explain below)*

Fingerprinting clearance required.

I certify that this duty statement represents an accurate description of the essential functions of this position.		I have read this duty statement and agree that it represents the duties I am assigned.	
SUPERVISOR'S SIGNATURE	DATE	EMPLOYEE'S SIGNATURE	DATE

SUPERVISION EXERCISED *(Check one)*:

☑ None ☐ Supervisor ☐ Lead Person ☐ Team Leader

FOR SUPERVISORY POSITIONS ONLY: Indicate the number of positions by classification that this position DIRECTLY supervises.

Total number of positions for which this position is responsible:

FOR LEADPERSONS OR TEAM LEADERS ONLY: Indicate the number of positions by classification that this position LEADS.

MISSION OF ORGANIZATIONAL UNIT:

Information System Division's (ISD) mission is to develop, support and promote the business value of IT which comes from the ability to conduct business processes more reliably, faster and at lower cost. ISD creates value by continually improving customer service and providing access to information that enables better decision making by CDSS business units.

ISD accomplishes this by:
- Effectively managing information systems and equipment;
- Planning, communicating and implementing responsible information technology policies and solutions; and,
- Sharing and transferring information technology knowledge and tools.

CONCEPT OF POSITION:

Under direction of the IT Supervisor II (IT Sup II), within the Information Systems Division (ISD) of the Department of Social Services (CDSS), the Information Technology Specialist I (IT Specialist I) is the Security Monitoring Specialist responsible for investigating, assessing and monitoring potential security vulnerabilities. Tasks include requiring regular innovative problem-solving, tracking remediation progress and creating actionable reports for cross-functional teams, planning, developing, and implementing technological information security solutions, security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments to address sources of disruption, ranging from natural disasters to malicious acts.

A. RESPONSIBILITIES OF POSITION:

40% Identifies, reviews, and analyzes network security appliance logs, Tier 1 Data Loss Prevention (DLP) alerts, audit logs, endpoint activity, email security events, cloud activity, and other data movement indicators to detect potential security incidents, unauthorized disclosure, improper transmission, misuse of data, or data exfiltration attempts. Monitors, investigates, triages, documents, and escalates DLP and data protection incidents involving sensitive, confidential, personal, or regulated information; identifies appropriate technical and business stakeholders to support incident response and resolution. Analyzes phishing, malware, endpoint protection, antimalware, DLP, vulnerability, configuration, and other security artifacts to assess risk, validate findings, identify trends, and recommend mitigation or remediation actions. Conducts vulnerability and data protection risk assessments by configuring approved scanning tools, coordinating scan schedules based on asset criticality, analyzing vulnerability scan results, reviewing security misconfigurations, and validating findings using network, endpoint, application, and security monitoring tools. Monitors public, vendor, governmental, and authorized threat intelligence sources for emerging vulnerabilities, threats, and indicators of compromise that may affect departmental systems. Reviews logs, DLP events, vulnerability data, configuration information, and related security telemetry to identify evidence of potential intrusion activity, attempted data exfiltration, systemic security issues, or control weaknesses. Performs technical impact and risk assessments and prepares findings, metrics, reports, and recommendations related to securi

25% Collaborates with senior ISPO staff and technical subject matter experts to ensure accurate root-cause analysis is conducted and appropriate remediation options are identified. Conducts vulnerability assessments of networks, applications, operating systems, and related technical environments using approved security assessment tools, procedures, and methodologies. Develops, tests, and maintains scripts, queries, dashboards, tool configurations, workflows, and documentation used to support vulnerability scanning, validation, analysis, and reporting. Analyzes vulnerability scan results and related security data to validate accuracy, identify false positives, assess risk and business impact, prioritize findings, and recommend remediation options. Evaluates, prepares, and disseminates threat advisories and vulnerability notifications to system owners and other stakeholders in a timely manner. Develops metrics, reports, and technical summaries on system security posture, threat activity, vulnerability exposure, remediation progress, and patch management status. Uses authorized security testing and assessment tools and techniques to evaluate the effectiveness of implemented controls, validate identified weaknesses, and provide insight into the organization’s threat and vulnerability environment.

15% Manage and track the remediation of identified vulnerabilities. Prepare internal incident reports to notify management and staff of security problems or production anomalies identified in the system logs corrective action plans are created and provided to CDSS staff for resolution. Develop metrics for security incidents, based upon pre-defined categorizations and assist in the development of reports and dashboards, utilizing CDSS security tools. Work with teams and staff within the Information Systems Division to ensure remediation and solution implementation coordination in relation to security vulnerabilities. Implement and configure vulnerability scanning solutions and identify and track vulnerabilities through the remediation process. Coordinate and monitor deployment of security patches on a timely basis. Conduct follow up activities to ensure the corrective action plans are implemented and the risks are mitigated in a timely manner. Communicate remediation status as required.

15% Support program leads with development, implementation and maintenance of Information Security tools including Security Information Event Management (SIEM), intrusion detection, and event logs for design and implementation of alerts, reports, and monitoring compliance. Participate in annual risk and technical standards compliance reviews for Systems and IT projects as needed. Conduct quality assurance monitoring of all system changes. Review network status to ensure production changes do not have a negative impact on the network. Validate production changes have been through the “change management process”.

5% Perform other duties as assigned within the scope of the classification.

B. SUPERVISION RECEIVED:

The Information Technology Specialist I (IT Specialist I) receives supervision from the Information Technology Supervisor II (IT Sup II) within the Information Security and Privacy Office.

C. ADMINISTRATIVE RESPONSIBILITY:

None

D. PERSONAL CONTACTS:

The IT Specialist I may have contact with staff at all levels of CDSS, other departments and control agencies, e.g., Health and Human Services Agency, Department of Finance, Department of General Services, Department of Health Care Services, Office of Systems Integration, Federal Agencies, California Department of Technology and local government organizations and stakeholders. The IT Specialist I also meets regularly with vendors and contractors.

E. ACTIONS AND CONSEQUENCES:

The IT Specialist I must perform due diligence and exercise good judgment in their duties. They must also perform due diligence and exercise good judgment when making recommendations. Failure to perform due diligence and exercise good judgment would have an adverse impact on ISD and the Department.

This position requires the incumbent maintain consistent and regular attendance.

F. OTHER INFORMATION:

Job requires operating a computer terminal approximately 80% of the time. This position is subject to fingerprinting and criminal record clearance by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) .

This position is subject to fingerprinting and criminal record clearance by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).